



ZTE Red Magic 11 Pro (NX809J) contains a vulnerability that allows non-privileged applications to trigger sensitive operations.

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-40002
State	PUBLISHED
Assigner	zte
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-17 08:16:18 UTC
Updated	2026-04-17 15:13:15 UTC
Description	Red Magic 11 Pro (NX809J) contains a vulnerability that allows non-privileged applications to trigger sensitive operations. T

Risk And Classification

Primary CVSS: v3.1 5 MEDIUM from psirt@zte.com.cn

CVSS: 3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:L

EPSS: 0.000050000 probability, percentile 0.002000000 (date 2026-04-19)

Problem Types: CWE-269 | CWE-269 CWE-269: Improper Privilege Management

Version	Source	Type	Score	Severity	Vector
3.1	psirt@zte.com.cn	Secondary	5	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	5	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:L

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ZTE	Red Magic 11 Pro NX809J	affected GEN_NEEA_NX809J V1.0.0B14MR1 V1.0.0B14MR1 custom	Not specified

References

Reference	Source	Link	Tags
support.zte.com.cn/zte-iccp-isupport-webui/bulletin/detail/8224335890517684583	psirt@zte.com.cn	support.zte.com.cn	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

Vendor Comments And Credit

Discovery Credit

CNA: Christopher Nelson (en)

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report